NEW CURVES WITH MANY POINTS OVER SMALL FINITE FIELDS

KARL RÖKAEUS

Abstract.[1] We use class field theory to search for curves with many rational points, finding a number of improvements of the old records. In particular, we settle the question of how many points a curve over $\mathbf{F}_2$ of genus 17 can have, by finding one with 18 points.

Background

Let q be a prime power and let g be a non-negative integer. Denote by $\mathrm{N}_q(g)$ the maximum number of rational points possible on a projective, smooth and geometrically irreducible curve of genus g, defined over the finite field $\mathbf{F}_q$; equivalently, the number of rational places possible in a global function field of genus g with full constant field $\mathbf{F}_q$. Interest in determining $\mathrm{N}_q(g)$ arose in the 1980's, among others with [6]. It has turned out to be a difficult task; it is still open even for curves of small genera over $\mathbf{F}_2$, starting with $g = 12, 14$ and 16. See [2] for an overview of the history of the problem and of different methods that has been used, and [4] for the current intervals in which $\mathrm{N}_q(g)$ in known to lie for $g \leq 50$. We perform a computer search for curves with many points over $\mathbf{F}_q$ for $q \leq 5$ using class field theory; this yields a curve that shows $\mathrm{N}_2(17) = 18$, and improves upon the lower bounds in a number of other cases.

The search was done using Magma [1]. We have formulated everything in terms of function fields (rather than curves), see [7] and [5].

Method

Notation. By a function field F/k we will always mean a global function field with full constant field k, i.e., k is algebraically closed in F. We write $\mathbf{P}_F$ for the set of places of F.

Class Field Theory. Let F/k be a function field, let D be an effective divisor of F and let $\mathrm{Cl}_D(F)$ (or just Cl_D) be the ray divisor class group modulo D of F, i.e., the group of divisors relatively prime to D modulo principal divisors congruent to 1 modulo D. There is an inclusion reversing correspondence between abelian extensions K/F with conductor $\leq D$, and subgroups $H \subset \mathrm{Cl}_D(F)$ of finite index, see [3]. For U a subgroup of Cl_D of finite index d, let F_U^D/F be the corresponding abelian extension. This extension has degree d; it is unramified outside of the support of D, where a place splits completely if and only if its image lies in U. When $S \subset \mathbf{P}_F$ is a set of places whose images in Cl_D generate U we also write F_S^D/F for F_U^D/F. This is then the largest abelian extension of F with conductor $\leq D$ such that all places in S split completely.

The ramification behavior of F_U^D/F at the places in $\mathrm{Supp}(D)$ can be computed from the images of H in $\mathrm{Cl}_{D'}(F)$ for $D' \leq D$. Algorithms for computing the ray class groups are given in [3], where it is also indicated how to compute the invariants of the class field. This is implemented in Magma [1].

Date: April 6, 2012.

[1]The author is supported by The Wenner-Gren Foundations Postdoctoral Grant

Organization of the Search. We work over $k = \mathbf{F}_q$ for $q = 2, 3, 4, 5$. Using Magma, for all function fields F of genus 1 and 2 and for various divisors D we construct $\mathrm{Cl}_D(F)$; for each rational place we take the quotient with the subgroup generated by it, list the subgroups of these finite quotients and pull them back to $\mathrm{Cl}_D(F)$. This way we get all abelian extensions K/F of conductor $\leq D$ in which at least one rational place splits completely (so that k is the full constant field of F). We compare this to the tables [4] and record the improvements that we find.

Results

In this section we state the new records that we found together with the intervals in which $\mathrm{N}_q(g)$ was previously known to lie. The details required to construct all the new curves we found are are given in the last section.

New entries for the tables over $\mathbf{F}_2$.

g	N	Interval
17	18	$[17, 18]$
45	36	$[33, 37]$

New entries for the tables over $\mathbf{F}_3$.

g	N	Interval
17	28	$[25, 30]$
22	33	$[30, 36]$
33	48	$[46, 49]$
46	60	$[55, 63]$

New entries for the tables over $\mathbf{F}_4$.

g	N	Interval
41	72	$[65, 78]$

New entries for the tables over $\mathbf{F}_5$.

g	N	Interval
8	24	$[22, 28]$
10	31	$[27, 33]$
12	36	$[33, 38]$
26	60	$[\ , 68]$
35	72	$[68, 85]$
37	80	$[72, 89]$
40	72	$[\ , 94]$
45	96	$[88, 104]$
46	81	$[75, 106]$

Details for the construction

In this section we give all details needed to construct the curves stated above. We begin by giving some of these constructions as detailed examples; then follows a list containing just the necessary details for each record.

To make it easy for the reader to check the result, below we use Magma's notation for representing function fields and places; the field F is represented as a finite separable extension of a rational function field $k(x)$. Every place of F then corresponds either to a prime ideal in the integral closure of $k[x]$ or one in the integral closure of the valuation ring of the degree valuation.

Example (Genus 17 over $\mathbf{F}_2$.). Let F be the hyperelliptic genus 2 field defined by $y^2 + (x^2 + x + 1)y + x^5 + x^4 + x^2 + x$ over the rational field $\mathbf{F}_2(x)$. Let $S = \{(1/x, y/x^3), (x + 1, y + 1)\}$ and let $P = (x + 1, y + x + 1)$. We get a sequence of fields $F \subset F_S^{2P} \subset F_S^{3P} \subset F_S^{5P}$.

First, Cl_{2P} is isomorphic to $\mathbf{Z}/28 \oplus \mathbf{Z}$. In it, S generates a subgroup of index 4. The field F_S^{2P} has genus 7 and 10 rational places, the best possible. (This was already known). We get an explicit equation for this extension as $T^4 + (x^3 + x)T^2 + (x^4 + 1)T + (x^6 + x^3 + x^2 + x)y + x^{16} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^5 + x^4 + 1$.

Next, Cl_{3P} is isomorphic to $\mathbf{Z}/56 \oplus \mathbf{Z}$. The subgroup generated by S in Cl_{3P} has index 8. The ray class field F_S^{3P} has genus 17 and 18 rational places. This is a new record and the best possible, showing that $\mathrm{N}_2(17) = 18$. We can also get an explicit equation for F_S^{3P} (which is somewhat messy and therefore left to the appendix). Using this we can construct the field without using class field theory, and then using Magma to compute its genus and number of rational places. This gives an independent verification that it really has genus 17 and 18 rational places.

Furthermore Cl_{5P} is isomorphic to $\mathbf{Z}/2 \oplus \mathbf{Z}/112 \oplus \mathbf{Z}$. The field F_S^{5P} has genus 45 and 34 rational places, the old record was 33 (in the next example we give one with 36 places).

Example (Genus 45 over $\mathbf{F}_2$). Take the genus two field given as an extension of $\mathbf{F}_2(x)$ by $y^2 + (x^3 + x + 1)y + x^6 + x^5 + x^4 + x^2$. It has 4 rational places and 3 places of degree 2; use two of the latter to construct the divisor $D = (x^2 + x + 1, y + x + 1) + 3(x^2 + x + 1, y + x^2 + x)$, and let U be generated by the images of the three rational places $\{(x, y + x), (x + 1, y), (x + 1, y + 1)\}$ in Cl_D. The index of U is 12 and F_U^D has genus 45 and 36 rational places, showing that $\mathrm{N}_2(45)$ equals either 36 or 37.

Example (Genus 22 and 46 over $\mathbf{F}_3$). Let F be given by $y^2 + 2x^6 + x^5 + 2x^4 + x^3 + 2x^2 + x + 2$, let $D = 2(1/x, y/x^3 + 1) + 2(x, y + 2)$ and let $S = \{(x + 1, y + x + 2), (x + 2, y + x), (x + 2, y + x + 1)\}$. The field F_S^D has genus 46 and 60 rational places. It has a subfield K of genus 22 with 33 rational places. By listing subgroups of Cl_D this is easy to find; however, if we want to express K as F_T^D for some set of places T, then we have to use places of rather high degree: The easiest way to obtain such T is to add the degree 5 place $(x^5 + x^3 + x + 1, y + 2x^4 + x^3 + 2x)$ to S. Then $K = F_T^D \subset F_S^D$.

Explicitly, F_T^D can be given as an extension of F by the equations

$$T_1^3 + 2T_1 + (x^3 + 2x^2 + x + 1 + 1/x)y + x^6 + 2x^2 + 2x + 1/x$$

$$T_2^3 + 2T_2 + (x^3 + 2x^2 + x + 2/x)y + x^6 + 2x^3 + 2x^2 + 2 + 2/x$$

which we also use to verify that it has the claimed genus and number of places.

List of data sufficient to construct each curve. Below we give sufficient details to construct each of the records that we found: For each entry first a finite field field $\mathbf{F}_q$ and a pair (g, N); then a global function field $F/\mathbf{F}_q$; then a divisor D of this function field; then a set S of rational places. The ray class field $F_S^D/\mathbf{F}_q$ then has genus g and N rational places. This can be proved using the algorithms for computing ray divisor class groups which are given in [3] and implemented for example in Magma. Also, in cases where it seems reasonable with respect to space we have included defining equation for the extension F_S^D/F, which we then also

have used to give an independent verification that the field really has the claimed genus and number of rational places.

Although Magma is a proprietary software, there is a calculator *magma.maths.usyd.edu.au/calc/* that is free to use and sufficient to construct the records from the details given below.

Details for the curves over $\mathbf{F}_2$.

- $\mathbf{F}_2$: $(g, N) = (17, 18)$

$$F : y^2 + (x^2 + x + 1)y + x^5 + x^4 + x^2 + x$$
$$D = 3(z + 1, y + z + 1)$$
$$S = \{(1/z, y/z^3), (z + 1, y + 1)\}.$$

Defining polynomial:

$$\begin{aligned}
&T^8+(x^5 + x^4 + x + 1)T^6 + (x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)T^5\\
&+((x^{17} + x^{15} + x^{14} + x^{13} + x^{12} + x^{10} + x^7 + x^5 + x + 1)y + (x^{22}\\
&+x^{20} + x^{19} + x^{14} + x^{12} + x^{11} + x^{10} + x^7 + x^5 + x^3 + x^2 + x))T^4\\
&+(x^{11} + x^{10} + x^9 + x^8 + x^3 + x^2 + x + 1)T^3\\
&+((x^{31} + x^{29} + x^{28} + x^{27} + x^{24} + x^{23} + x^{21}\\
&+x^{16} + x^{13} + x^{10} + x^9 + x^5 + x^4 + x^3 + x^2 + x)y\\
&+(x^{35} + x^{32} + x^{31} + x^{30} + x^{29} + x^{27} + x^{26} + x^{25} + x^{24}\\
&+x^{19} + x^{15} + x^{12} + x^{10} + x^6 + x^5 + x^4 + x^3 + x))T^2\\
&+((x^{33} + x^{30} + x^{28} + x^{27} + x^{26} + x^{25} + x^{24} + x^{23}\\
&+x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{15} + x^{14} + x^{13}\\
&+x^{12} + x^{11} + x^9 + x^4 + x^3 + 1)y + (x^{37} + x^{35} + x^{34}\\
&+x^{33} + x^{30} + x^{24} + x^{23} + x^{16} + x^{15} + x^{13} + x^6 + x^3 + x^2 + x))T\\
&+(x^{54} + x^{53} + x^{51} + x^{50} + x^{47} + x^{45} + x^{44} + x^{43} + x^{42}\\
&+x^{41} + x^{39} + x^{38} + x^{37} + x^{36} + x^{29} + x^{24} + x^{22} + x^{19} + x^{17} + x^{16}\\
&+x^{15} + x^{11} + x^{10} + x^7 + x^6 + x^2)y + x^{60} + x^{58} + x^{57} + x^{55} + x^{54}\\
&+x^{53} + x^{52} + x^{51} + x^{47} + x^{46} + x^{45} + x^{40} + x^{39} + x^{37} + x^{35} + x^{33}\\
&+x^{32} + x^{30} + x^{29} + x^{28} + x^{26} + x^{21} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15}\\
&+x^{13} + x^{11} + x^9 + x^6 + x^4 + x^2 + 1.
\end{aligned}$$

- $\mathbf{F}_2$: $(g, N) = (45, 36)$

$$F : y^2 + (x^3 + x + 1)y + x^6 + x^5 + x^4 + x^2$$
$$D = (x^2 + x + 1, y + x + 1) + 3(x^2 + x + 1, y + x^2 + x).$$
$$S = \{(x, y + x), (x + 1, y), (x + 1, y + 1)\}.$$

Details for the curves over $\mathbf{F}_3$.

- $\mathbf{F}_3$: $(g, N) = (17, 28)$

$$F : y^2 + x^5 + x^4 + x^2 + 2x$$
$$D = (1/x, y/x^3) + (x + 1, y + 1) + 2(x^2 + 1, y)$$
$$S = \{(x + 1, y + 2), (x + 2, y + 1), (x + 2, y + 2)\}.$$

Defining polynomials:

$$T_1^4 + (x^3 + x)T_1^2 + 2x^6 + 2x^5 + x^4 + 2x^3 + 2x^2$$
$$T_2^2 + (x + 1)y + x^3 + x^2 + x + 1$$

- $\mathbf{F}_3$: $(g, N) = (22, 33)$

$$F : y^2 + 2x^6 + x^5 + 2x^4 + x^3 + 2x^2 + x + 2$$
$$D = 2(1/x, y/x^3 + 1) + 2(x, y + 2)$$
$$S = \{(x + 1, y + x + 2), (x + 2, y + x), (x + 2, y + x + 1),$$
$$(x^5 + x^3 + x + 1, y + 2x^4 + x^3 + 2x)\}.$$

Defining polynomials:

$$T_1^3 + 2T_1 + (x^3 + 2x^2 + x + 1 + 1/x)y + x^6 + 2x^2 + 2x + 1/x$$
$$T_2^3 + 2T_2 + (x^4 + 2x^3 + x^2 + 2)y/x + (x^7 + 2x^4 + 2x^3 + 2x + 2)/x$$

- $\mathbf{F}_3$: $(g, N) = (33, 48)$

$$F : y^2 + 2x^6 + x^5 + 2x^4 + x$$
$$D = (x^2 + 1, y + x + 2) + (x^2 + 1, y + 2x + 1)$$
$$S = \{(1/x, y/x^3 + 1), (1/x, y/x^3 + 2), (x, y)\}.$$

- $\mathbf{F}_3$: $(g, N) = (46, 60)$

$$F : y^2 + 2x^6 + x^5 + 2x^4 + x^3 + 2x^2 + x + 2$$
$$D = 2(1/x, y/x^3 + 1) + 2(x, y + 2)$$
$$S = \{(x + 1, y + x + 2), (x + 2, y + x), (x + 2, y + x + 1)\}.$$

Details for the curves over $\mathbf{F}_4$. Below, a is a primitive element of $\mathbf{F}_4$.

- $\mathbf{F}_4$: $(g, N) = (41, 72)$

$$F : y^2 + (x^2 + x)y + x^5 + x^3 + a^2x^2 + a^2x$$
$$D = (x + a, y + x) + (x + a, y + a^2)$$
$$S = \{(1/x, y/x^3), (x, y), (x + 1, y)\}.$$

Details for the curves over $\mathbf{F}_5$.

- $\mathbf{F}_5$: $(g, N) = (8, 24)$

$$F : y^2 + 4z^6 + 2z^5 + 2z^3 + z^2 + 2z$$
$$D = (z^2 + 2z + 3, y + 4z + 4) + (z^2 + 4z + 2, y + 3z + 2)$$
$$S = \{(1/z, y/z^3 + 1), (1/z, y/z^3 + 4), (z, y), (z + 3, y + 4),$$
$$(z + 1, y + 4), (z + 2, y + 2), (z + 4, y + 2), (z + 4, y + 3)\}.$$

Defining polynomial:

$$T^3 + ((4z + 3)y + (3z^4 + 3z^2 + 2))T$$
$$+ (4z^3 + 3z^2 + 4z + 2)y + 4z^6 + z^4 + z^3 + z^2 + 2z + 2.$$

- $\mathbf{F}_5$: $(g, N) = (10, 31)$

$$F : y^2 + 4z^6 + 2z^5 + 3z^3 + 4z^2 + 1$$
$$D = 3(z + 3, y + z)$$
$$S = \{(1/z, 1/z^3 y + 1), (1/z, y/z^3 + 4), (z, y + z + 2), (z + 3, y + z + 1), (z + 1, y + 1), (z + 4, y + 4)\}.$$

Defining polynomial:

$$T^5 + 4T + (4z^3 + z^2 + 3z + 4)y/(z + 3) + + (z^6 + 3z^5 + 4z^2 + 2z + 3)/(z + 3)$$

- $\mathbf{F}_5$: $(g, N) = (12, 36)$

$$F : y^2 + 3z^6 + z^5 + 2z^4 + 4z^3 + 4z^2 + 3z + 4$$
$$D = 2(1/z)$$
$$S = \{(z, y + 1), (z, y + 4), (z + 2, y + z + 3), (z + 2, y + z + 1), (z + 4, y + 2), (z + 4, y + 3)\}.$$

Defining polynomials:

$$x^2 + 4z^3 + 2z^2 + 4z + 1$$
$$w^3 + (3z^3 + z^2 + 2z + 1)w + z^5 + 3z^3 + 3z$$

- $\mathbf{F}_5$: $(g, N) = (26, 60)$

$$F : y^2 + z^6 + z^5 + 4z^4 + 4z^3 + 4z^2 + z + 1$$
$$D = (z^2 + z + 1, y + 3) + (z^2 + 3, y + 3z + 2)$$
$$S = \{(1/z, y/z^3 + 2), (z, y + 2), (z + 3, y + z), (z + 2, y + 4)\}.$$

- $\mathbf{F}_5$: $(g, N) = (35, 72)$

$$F : y^2 + z^6 + 4z^5 + 2z^4 + 2z^2 + 4z + 1$$
$$D = (z^2 + z + 1, y + 2) + (z + 1)$$
$$S = \{(1/z, y/z^3 + 2), (z, y + 2), (z + 3, y + 2), (z + 2, y + z + 1), (z + 4, y + 1), (z + 4, y + 4)\}.$$

- $\mathbf{F}_5$: $(g, N) = (37, 80)$

$$F : y^2 + z^5 + z^4 + 2z^3 + z^2 + 4z$$
$$D = 3(z, y)$$
$$S = \{(1/z, y/z^3), (z + 1, y), (z + 4, y + 1), (z + 4, y + 4)\}.$$

- $\mathbf{F}_5$: $(g, N) = (40, 72)$

$$F : y^2 + 2z^5 + z^4 + 2$$
$$D = (z + 3) + (z)$$
$$S = \{(1/z, y/z^3), (z + 1, y + 2), (z + 1, y + 3), (z + 4, y)\}.$$

- $\mathbf{F}_5$: $(g, N) = (45, 96)$

$$F : y^2 + 2z^6 + 4z^4 + 3z^2 + 1$$
$$D = 2(1/z)$$
$$S = \{(z+3, y), (z+1, y), (z+2, y), (z+4, y)\}.$$

- $\mathbf{F}_5$: $(g, N) = (46, 81)$

$$F : y^2 + z^6 + 2z^5 + 2z^4 + z^3 + 2z^2 + 2z + 1$$
$$D = 2(z^2 + 4z + 2, y + z^2 + 4)$$
$$S = \{(z, y+2), (z+3, y+3), (z+1, y+3)\}.$$

Acknowledgments. The author thanks the Wenner-Gren Foundations for financial support; the Korteweg-de Vries Institute at the University of Amsterdam for hospitality; and Gerard van der Geer for his hospitality and for helpful conversations and comments.

References

[1] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput., 24 (1997), 235–265.

[2] G. van der Geer and M. van der Vlugt, *Tables of curves with many points*, Math. Comp 69, (2000), no 230 pp. 797–810

[3] F. Hess and S. Pauli and M.E. Pohst, *Computing the multiplicative group of residue class rings*, Math. Comp. 72 (2003) 1531–1548 (electronic)

[4] *manYPoints–Table of Curves with Many Points*, Tables of upper and lower bounds for the maximum number of points on a genus g curve over different finite fields. Moderators: G. van der Geer, E. Howe, K. Lauter, C. Ritzenthaler, *Address:* `www.manypoints.org`

[5] H. Niederreiter; C. P. Xing, *Rational Points on Curves over Finite Fields*, LMS Lecture Note Series 285, 2001

[6] J-P. Serre, *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*, C. R. Acad. Sci. Paris Sér. I Math. 296, Serie I (1983), p. 397-402. (= Oeuvres III, No. 128, p. 658-663).

[7] H. Stichtenoth, *Algebraic function fields and codes*, Graduate Texts in Mathematics 254, Springer-Verlag, 2009

Karl Rökaeus, Korteweg de Vries Instituut voor Wiskunde, Universiteit van Amsterdam, P.O. Box 94248, 1090 GE Amsterdam, The Netherlands

E-mail address: `S.K.F.Rokaeus@uva.nl`